AAA ルールの設定

この章では、ネットワーク アクセスに対して AAA（トリプル エー）をイネーブルにする方法について説明します。

管理アクセスの AAA については、P.11-2 の「AAA Access」を参照してください。

この章には、次の項があります。

AAA パフォーマンス

セキュリティ アプライアンスは「カットスルー プロキシ」を使用します。この方法により、従来のプロキシ サーバと比較して、パフォーマンスが大幅に向上します。従来のプロキシ サーバは、OSI モデルのアプリケーション レイヤですべてのパケットを分析するため、プロキシ サーバのパフォーマンスに負担がかかります。セキュリティ アプライアンス カットスルー プロキシは、アプリケーション レイヤで最初にユーザ確認を行い、標準 AAA サーバまたはローカル データベースで認証します。セキュリティ アプライアンスはユーザを認証した後、セッション フローをシフトするため、セッション ステート情報を維持したまま、すべてのトラフィックが送信元と宛先の間で直接かつ迅速に流れます。

AAA ルールの設定

この項では、AAA ルールを設定する方法について説明します。次の項目を取り上げます。

AAA Rules

Configuration > Security Policy > AAA Rules

Security Policy ペインには、ルールで表現されたネットワーク セキュリティ ポリシーが表示されます。このウィンドウには、他のルール用のタブとともに、AAA ルール用のタブがあります。この項目では AAA ルールを説明します。AAA サービスの概要については、第 10 章「AAA サーバの設定」を参照してください。

AAA Rules タブを選択すると、MAC 免除ルールとともに、認証、認可、またはアカウンティング（AAA）ルールを定義できます。AAA はセキュリティ アプライアンスに、ユーザが誰か、ユーザが何を実行できるか、およびユーザが何を実行したかを知らせます。認証のみで使用することも、認可とともに使用することもできます。認可には常に認証が必要です。たとえば、内部ネットワークのサーバにアクセスする外部ユーザを認証する場合、認証だけで十分に対応します。ただし、特定のユーザがアクセスする内部サーバを制限する場合は、認可サーバを設定し、どのサーバとサービスにユーザがアクセスできるのかを指定することができます。

AAA には、ユーザ アクセスに対して、アクセスリストのみを使用する場合よりもレベルの高い保護および制御機能が用意されています。たとえば、すべての外部ユーザが DMZ ネットワークのサーバにアクセスできるようにするアクセスリストを作成できます。登録したユーザだけがサーバに Telnet できるようにするには、AAA を設定して、認証または認可、あるいはその両方が行われたユーザだけがセキュリティ アプライアンスを通過できるようにします。サーバに独自の認証および認可がある場合、ユーザは 2 番目のユーザ名とパスワードのセットを入力します（FTP の場合、ユーザはアット マーク（@）で区切ったユーザ名とパスワードの両方を入力する必要があります）。

各 AAA ルールでは、一致トラフィックの次の特性が識別されます。

- 送信元および宛先ネットワーク
- アクション（認証、認可、またはアカウンティング。ルールでは、AAA から MAC アドレスを除外することもできます）
- AAA サーバ グループ
- サービス グループ（Telnet や FTP など）

制約事項

ASDM は、次の AAA ルールの混合構成をサポートしていません。

- 送信元および宛先アドレスの指定
- 送信元および宛先アドレスのアクセスリストの照合

  コンフィギュレーションにすでに AAA ルールが含まれている場合、追加できるのは同じ種類の AAA ルールのみです。AAA ルールを設定していない場合、ASDM ではアクセスリストに一致するルールのみを追加できます。ルールがアクセスリストに一致するように変換するには、ASDM の AAA ルールをすべて削除し、再度追加する必要があります（このときルールは設定せず、ASDM ではアクセスリスト モードのデフォルト値となります）。ASDM では、どちらのモードでも AAA ルールのコンフィギュレーションは同じです。

- FTP 認証の場合、ユーザは次の形式で名前とパスワードを入力する必要があります。

  セキュリティ アプライアンス *_name@ftp_name*
  セキュリティ アプライアンス *_password@ftp_password*
- セキュリティ アプライアンスで認証が正常に行われた後、セキュリティ アプライアンスは FTP 名とパスワードを FTP サーバに転送します。Telnet および HTTP（認証用に設定されている場合）など他のサービスでは、宛先サーバのプロンプトで 2 番目の名前とパスワードを入力する必要があります。
- メールまたは SMTP など、一部のサービスの認証は確実ではありません。すべてのサービスで認証を必要とするように指定する場合、ユーザをまず Telnet、FTP、HTTP、または HTTPS（または確実に認証プロンプトを提供するその他のサービス）で認証し、次に他のサービスで認証する必要があります。
- AAA 認可ルールは TACACS+ サーバをサポートしますが、他のサーバはサポートしません。ただし、ローカル データベースを使用して、セキュリティ アプライアンス コマンドに対してユーザを認可することはできます。
- AAA アカウンティング ルールは、AAA Server Group としてのローカル データベースの使用をサポートしていません。

前提条件

1. Configuration > Features > Properties > AAA Setup > AAA Server Groups ペインで、各ホストまたはサーバを定義します。
2. ローカル データベースにユーザを追加します （Configuration > Features > Properties > Administration > User Accounts を参照）。
3. ユーザが指定したネットワークにアクセスできることを確認します（必要に応じて「Access Rules」を参照）。
4. AAA サーバを正しくセットアップします。

フィールド

- Add：新しい AAA ルールを追加します。追加するルールのタイプをドロップダウン リストから選択します。
- Edit：AAA ルールを編集します。
- Delete：AAA ルールを削除します。
- Move Up：ルールを上に移動します。ルールは、テーブルに表示されている順に査定されます。したがって、重複するルールがある場合、その順序が問題になります。
- Move Down：ルールを下に移動します。
- Cut：ルールを切り取ります。
- Copy：ルールのパラメータをコピーします。Paste ボタンを使用すれば、新しいルールを同じパラメータで開始できます。
- Paste：コピーまたは切り取ったルールのパラメータがあらかじめ入力された Add/Edit Rule ダイアログボックスが開きます。そこでルールを変更し、テーブルに追加します。Paste ボタンでは、ルールが選択したルールの上に追加されます。Paste ドロップダウン リストで使用可能な Paste After 項目では、ルールが選択したルールの後ろに追加されます。
- Find：一致するルールだけを表示するように、表示内容をフィルタリングします。Find をクリックすると、Filter フィールドが開きます。もう 1 回 Find をクリックすると、Filter フィールドが非表示になります。
  - Filter ドロップダウン リスト：フィルタリングする基準を、Interface、Source、Destination、Service、Action、または Rule Query のいずれかから選択します。ルール クエリーとは、複数の基準の集合で、保存して繰り返し使用できます。
  - Filter フィールド：Interface タイプの場合、このフィールドはドロップダウン リストになり、インターフェイス名または **All Interfaces** を選択できます。Action タイプの場合、ドロップダウン リストには Permit と Deny が表示されます。Rule Query タイプの場合、ドロップダウン リストにはすべての定義済みルール クエリーが含まれます。Source および

Destination タイプの場合は、IP アドレスを受け入れます。IP アドレスを 1 つ手動で入力するか、... ボタンをクリックし、Browse Address ダイアログボックスを開いて参照します。Service タイプの場合は、TCP、UDP、TCP-UDP、ICMP、または IP プロトコル タイプを受け入れます。IP アドレスを 1 つ手動で入力するか、... ボタンをクリックし、Browse Service Groups ダイアログボックスを開いて参照します。

  - Filter：フィルタリングを実行します。
  - Clear：Filter フィールドをクリアします。
  - Rule Query：名前付きルール クエリーを管理できる Rule Queries ダイアログボックスが開きます。

- Show Rule Flow Diagram：ルール テーブルの下に Rule Flow Diagram 領域を表示します。この図では、ネットワーク、トラフィックのタイプ、インターフェイス名、フローの方向、およびアクション（Authenticate または Do Not Authenticate など）を示しています。
- Packet Trace：選択したルールの特性と共にパラメータがあらかじめ入力された Packet Tracer ツールを開きます。

次の説明では、AAA Rules テーブルのカラムをまとめています。テーブル セルをダブルクリックすると、カラムの内容を編集できます。カラム ヘッダーをダブルクリックすると、選択したカラムが並び替えキーとして使用され、テーブルが英数字の昇順に並び替わります。ルールを右クリックすると、Insert および Insert After 項目と共に、ボタンで表されているオプションがすべて上に表示されます。これらの項目では、選択したルールの前に新しいルールが挿入されるか（Insert）、選択したルールの後ろに新しいルールが挿入されます（Insert After）。

- No：ルールの評価順序を示します。
- Enabled：ルールがイネーブルになっているか、またはディセーブルになっているかを示します。
- Action：AAA ルールのタイプを指定します。
- Source：Destination カラムに一覧表示された IP アドレスにトラフィックが送信されたとき、AAA の対象となる IP アドレスを一覧表示します。
- Destination：Source カラムに一覧表示された IP アドレスからトラフィックが送信されたとき、AAA の対象となる IP アドレスを一覧表示します。
- Service：ルールで指定されるサービスまたはプロトコルを表示します。
- Action：Authenticate、Do Not Authenticate、Authorize、Do Not Authorize など、ルールで指定されたアクションを表示します。
- Server Group：AAA Server Group タグを指定します。AAA サーバ グループの設定は、Properties > AAA Setup > AAA Server Groups で行います。新しい AAA ルールを作成するには、サーバ グループがあり、その中に 1 つ以上のサーバが存在する必要があります。
- Time：このルールで有効な時間範囲の名前を指定します。
- Description：ルールを追加したときに入力した説明です。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

認証ルールの追加および編集

セキュリティ アプライアンスでは、AAA サーバまたはローカル データベースを使用するネットワーク アクセス認証を設定できます。

所定の IP アドレスのユーザは、認証セッションが期限切れになるまで、すべてのルールおよびタイプに対して一度だけ認証を受ける必要があります（タイムアウト値については、「Timeouts」を参照）。たとえば、Telnet および FTP を認証するようにセキュリティ アプライアンスが設定されていて、ユーザが正常に Telnet 認証を受けた場合、認証セッションが継続している限り、ユーザは FTP 認証を受ける必要はありません。

プロトコルまたはサービスへのネットワーク アクセス認証を要求するようにセキュリティ アプライアンスを設定することは、すべてのプロトコルまたはサービスについて可能ですが、ユーザが直接認証を受けることができるのは、HTTP（S）、Telnet、または FTP だけです。ユーザがこれらのサービスのいずれかの認証を受けないと、セキュリティ アプライアンスは認証が必要な他のトラフィックを許可しません。

セキュリティ アプライアンスで HTTP（S）、Telnet、または FTP は許可しないが、他のタイプのトラフィックは認証する場合、仮想 Telnet を設定します。仮想 Telnet では、セキュリティ アプライアンス上に設定された所定の IP アドレスにユーザが Telnet 接続すると、セキュリティ アプライアンスは Telnet プロンプトを表示します。

Telnet、HTTP（S）、および FTP の場合、セキュリティ アプライアンスは認証プロンプトを生成します。宛先サーバにも独自の認証がある場合、ユーザは別のユーザ名とパスワードを入力します。

HTTP 認証では、スタティック NAT が設定されている場合、セキュリティ アプライアンスはローカル ポートをチェックします。セキュリティ アプライアンスは、グローバル ポートにかかわらず、ローカル ポート 80 を宛先とするトラフィックを検出した場合、HTTP 接続を代行受信し、認証を実行します。

たとえば、外部 TCP ポート 889 はポート 80（www）に変換され、すべての関連アクセスリストはトラフィックを許可するものとします。

この場合、ユーザはポート 889 で 10.48.66.155 にアクセスを試み、セキュリティ アプライアンスはそのトラフィックを代行受信し、HTTP 認証を実行します。セキュリティ アプライアンスが HTTP 接続の完了を許可する前に、ユーザの Web ブラウザには HTTP 認証ページが表示されます。

ローカル ポートがポート 80 以外の場合、ユーザには認証ページが表示されません。その代わりに、セキュリティ アプライアンスは、要求したサービスを使用するには認証を受ける必要があることを示すエラーメッセージを Web ブラウザに送信します。

（注） HTTP クライアント認証（「高度な AAA 機能の設定」を参照）を使用せずに HTTP 認証を使用する場合、ユーザ名とパスワードはクリア テキストで宛先 Web サーバに送信され、AAA サーバには送信されません。たとえば、内部ユーザが外部の Web サーバにアクセスするときに認証すると、有効なユーザ名とパスワードが外部から判別可能になります。HTTP 認証をイネーブルにする場合は、必ずセキュアな HTTP クライアント認証を使用することをお勧めします。

FTP の場合、セキュリティ アプライアンス ユーザ名、アット マーク（@）、FTP ユーザ名（name1@name2）を入力するオプションがあります。パスワードには、セキュリティ アプライアンス パスワード、アット マーク（@）、FTP パスワード（password1@password2）を入力します。たとえば、次のテキストを入力します。

```
name> jamiec@jchrichton
password> letmein@he110
```

この機能は、複数のログインを必要とするファイアウォールをカスケード接続している場合に有用です。複数の名前およびパスワードは、複数のアット マーク（@）で区切ることができます。

フィールド

Interface and Action：インターフェイス、アクション、および AAA サーバ グループを選択します。

- Interface：このルールを適用するインターフェイスを選択します。
- Action：**Authenticate** または **Do not Authenticate** を選択します。
- AAA Server Group：AAA サーバ グループまたはローカル データベースを選択します。Properties > AAA Setup > AAA Server Groups でサーバ グループを追加する必要があります。
- Add Server/User：サーバを選択した AAA サーバ グループに追加するか、ユーザをローカル データベースに追加するには、このボタンをクリックします。

Source：認証するトラフィックの送信元アドレスを指定します。

- Type：any、IP アドレス、Network Object Group、または Interface IP など、使用するアドレスのタイプを選択します。

  IP address を選択した場合、次のフィールドが表示されます。

  - IP Address：手動で入力するか、**...** ボタンをクリックして、Browse Address ダイアログボックスから選択します。
  - Netmask：ドロップダウン リストからサブネット マスクを選択します。

  Network Object Group を選択した場合、次のフィールドが表示されます。

  - Group Name：ドロップダウン リストからグループ名を選択するか、**...** ボタンをクリックして Browse Address ダイアログボックスを開きます。Browse Address ダイアログボックスでは、ネットワーク オブジェクト グループを追加できます。

  Interface IP を選択した場合、次のフィールドが表示されます。

  - Interface：ドロップダウン リストからインターフェイスを選択します。

Destination：認証するトラフィックの宛先アドレスを指定します。

- Type：any、IP アドレス、Network Object Group、または Interface IP など、使用するアドレスのタイプを選択します。

  IP アドレスを選択した場合、次のフィールドが表示されます。

  - IP Address：手動で入力するか、**...** ボタンをクリックして、Browse Address ダイアログボックスから選択します。
  - Netmask：ドロップダウン リストからサブネット マスクを選択します。

  Network Object Group を選択した場合、次のフィールドが表示されます。

  - Group Name：ドロップダウン リストからグループ名を選択するか、**...** ボタンをクリックして Browse Address ダイアログボックスを開きます。Browse Address ダイアログボックスでは、ネットワーク オブジェクト グループを追加できます。

  Interface IP を選択した場合、次のフィールドが表示されます。

  - Interface：ドロップダウン リストからインターフェイスを選択します。

Protocol and Service：認証するトラフィックのポートまたはプロトコルを指定します。

- Protocol：tcp、udp、ip、icmp、またはその他のいずれかのトラフィックのプロトコルを選択します。

  tcp または **udp** を選択した場合、次のフィールドが表示されます。

  - Source Port：認証するトラフィックの送信元ポートを設定します。

    Service：ポートまたはポートの範囲を入力するには、このオプション ボタンをクリックします。ドロップダウン リストから、=（等しい）、!=（等しくない）、>（大きい）、<（小さい）などの演算子および範囲を選択します。数字を入力するか、ドロップダウン リストからウェルノウン ポート名を選択します。範囲の場合、数字を指定する必要があります。

    Group：Service Groups で作成されたサービス グループを指定するには、このオプション ボタンをクリックします。ドロップダウン リストからグループ名を選択するか、**...** ボタンをクリックして Browse Service Groups ダイアログボックスを開きます。Browse Service Groups ダイアログボックスでは、サービス グループを追加できます。

- Destination Port：認証するトラフィックの宛先ポートを設定します。

  Service：ポートまたはポートの範囲を入力するには、このオプション ボタンをクリックします。ドロップダウン リストから、=（等しい）、!=（等しくない）、>（大きい）、<（小さい）などの演算子および範囲を選択します。数字を入力するか、ドロップダウン リストからウェルノウン ポート名を選択します。範囲の場合、数字を指定する必要があります。

  Group：Service Groups で作成されたサービス グループを指定するには、このオプション ボタンをクリックします。ドロップダウン リストからグループ名を選択するか、**...** ボタンをクリックして Browse Service Groups ダイアログボックスを開きます。Browse Service Groups ダイアログボックスでは、サービス グループを追加できます。

icmp を選択した場合、次のフィールドが表示されます。

- ICMP Type：ICMP タイプを入力するには、このオプション ボタンをクリックします。数字を入力するか、ドロップダウン リストからウェルノウン タイプを選択します。
- ICMP Group：Service Groups で作成されたサービス グループを指定するには、このオプション ボタンをクリックします。ドロップダウン リストからグループ名を選択するか、**...** ボタンをクリックして Browse Service Groups ダイアログボックスを開きます。Browse Service Groups ダイアログボックスでは、サービス グループを追加できます。

other を選択した場合、次のフィールドが表示されます。

- Protocol：IP プロトコル タイプを入力するには、このオプション ボタンをクリックします。数字を入力するか、ドロップダウン リストからウェルノウン タイプを選択します。
- Protocol Group：Service Groups で作成されたサービス グループを指定するには、このオプション ボタンをクリックします。ドロップダウン リストからグループ名を選択するか、**...** ボタンをクリックして Browse Service Groups ダイアログボックスを開きます。Browse Service Groups ダイアログボックスでは、サービス グループを追加できます。

Rule Flow Diagram：このルールの Rule Flow Diagram を表示します。この図では、ネットワーク、トラフィックのタイプ、インターフェイス名、フローの方向、およびアクション（Authenticate または Do Not Authenticate など）を示しています。

Options：このルールのオプションを設定します。

- Time Range：ドロップダウン リストから既存の時間範囲の名前を選択します。時間範囲では、指定した時間だけルールがイネーブルになります。時間範囲は「時間範囲の設定」で作成します。
- Description：このルールの説明を入力します。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

認可ルールの追加および編集

TACACS+ でネットワーク アクセス認可を実行するように、セキュリティ アプライアンスを設定できます。

（注）　RADIUS を使用してユーザによるネットワーク アクセスを認証するようにセキュリティ アプライアンスを設定するとき、RADIUS 認可も暗黙にイネーブルになります。RADIUS 認可は、TACACS+ のような別の認可ルールを必要としません。認可での RADIUS の使用の詳細については、P.19-16 の「認可のための RADIUS サーバの設定」を参照してください。

認証ルールと認可ルールは互いに依存しませんが、認可ルールで一致した未認証トラフィックはすべて拒否されます。認可が成功するためには、ユーザは最初にセキュリティ アプライアンスで認証を受ける必要があります。所定の IP アドレスのユーザは、すべてのルールおよびタイプに対して一度だけ認証を受ければよいため、認証セッションが期限切れになっていなければ、トラフィックが認証文で一致した場合でも、認可が発生することがあります。

ユーザの認証が完了すると、セキュリティ アプライアンスは、一致するトラフィックの認可ルールをチェックします。トラフィックが認可ルールに一致した場合、セキュリティ アプライアンスはユーザ名を TACACS+ サーバに送信します。TACACS+ サーバはセキュリティ アプライアンスに応答し、ユーザ プロファイルに基づいてそのトラフィックの許可または拒否を示します。セキュリティ アプライアンスは、その応答内の認可ルールを実施します。

ユーザに対するネットワーク アクセス認可の設定については、ご使用の TACACS+ サーバのマニュアルを参照してください。

フィールド

Interface and Action：インターフェイス、アクション、および AAA サーバ グループを選択します。

- Interface：このルールを適用するインターフェイスを選択します。
- Action：**Authorize** または **Do not Authorize** を選択します。
- AAA Server Group：AAA サーバ グループまたはローカル データベースを選択します。Properties > AAA Setup > AAA Server Groups でサーバ グループを追加する必要があります。
- Add Server/User：サーバを選択した AAA サーバ グループに追加するか、ユーザをローカル データベースに追加するには、このボタンをクリックします。

Source：認可するトラフィックの送信元アドレスを指定します。

- Type：any、IP アドレス、Network Object Group、または Interface IP など、使用するアドレスのタイプを選択します。

  IP address を選択した場合、次のフィールドが表示されます。

  - IP Address：手動で入力するか、**...** ボタンをクリックして、Browse Address ダイアログボックスから選択します。
  - Netmask：ドロップダウン リストからサブネット マスクを選択します。

  Network Object Group を選択した場合、次のフィールドが表示されます。

  - Group Name：ドロップダウン リストからグループ名を選択するか、**...** ボタンをクリックして Browse Address ダイアログボックスを開きます。Browse Address ダイアログボックスでは、ネットワーク オブジェクト グループを追加できます。

  Interface IP を選択した場合、次のフィールドが表示されます。

  - Interface：ドロップダウン リストからインターフェイスを選択します。

Destination：認可するトラフィックの宛先アドレスを指定します。

- Type：any、IP アドレス、Network Object Group、または Interface IP など、使用するアドレスのタイプを選択します。

  IP address を選択した場合、次のフィールドが表示されます。

  - IP Address：手動で入力するか、**...** ボタンをクリックして、Browse Address ダイアログボックスから選択します。
  - Netmask：ドロップダウン リストからサブネット マスクを選択します。

  Network Object Group を選択した場合、次のフィールドが表示されます。

  - Group Name：ドロップダウン リストからグループ名を選択するか、**...** ボタンをクリックして Browse Address ダイアログボックスを開きます。Browse Address ダイアログボックスでは、ネットワーク オブジェクト グループを追加できます。

  Interface IP を選択した場合、次のフィールドが表示されます。

  - Interface：ドロップダウン リストからインターフェイスを選択します。

Protocol and Service：認可するトラフィックのポートまたはプロトコルを指定します。

- Protocol：tcp、udp、ip、icmp、またはその他のいずれかのトラフィックのプロトコルを選択します。

  tcp または **udp** を選択した場合、次のフィールドが表示されます。

  - Source Port：認可するトラフィックの送信元ポートを設定します。

    Service：ポートまたはポートの範囲を入力するには、このオプション ボタンをクリックします。ドロップダウン リストから、=（等しい）、!=（等しくない）、>（大きい）、<（小さい）などの演算子および範囲を選択します。数字を入力するか、ドロップダウン リストからウェルノウン ポート名を選択します。範囲の場合、数字を指定する必要があります。

    Group：Service Groups で作成されたサービス グループを指定するには、このオプション ボタンをクリックします。ドロップダウン リストからグループ名を選択するか、**...** ボタンをクリックして Browse Service Groups ダイアログボックスを開きます。Browse Service Groups ダイアログボックスでは、サービス グループを追加できます。
  - Destination Port：認可するトラフィックの宛先ポートを設定します。

    Service：ポートまたはポートの範囲を入力するには、このオプション ボタンをクリックします。ドロップダウン リストから、=（等しい）、!=（等しくない）、>（大きい）、<（小さい）などの演算子および範囲を選択します。数字を入力するか、ドロップダウン リストからウェルノウン ポート名を選択します。範囲の場合、数字を指定する必要があります。

    Group：Service Groups で作成されたサービス グループを指定するには、このオプション ボタンをクリックします。ドロップダウン リストからグループ名を選択するか、**...** ボタンをクリックして Browse Service Groups ダイアログボックスを開きます。Browse Service Groups ダイアログボックスでは、サービス グループを追加できます。

  icmp を選択した場合、次のフィールドが表示されます。

  - ICMP Type：ICMP タイプを入力するには、このオプション ボタンをクリックします。数字を入力するか、ドロップダウン リストからウェルノウン タイプを選択します。
  - ICMP Group：Service Groups で作成されたサービス グループを指定するには、このオプション ボタンをクリックします。ドロップダウン リストからグループ名を選択するか、**...** ボタンをクリックして Browse Service Groups ダイアログボックスを開きます。Browse Service Groups ダイアログボックスでは、サービス グループを追加できます。

  other を選択した場合、次のフィールドが表示されます。

  - Protocol：IP プロトコル タイプを入力するには、このオプション ボタンをクリックします。数字を入力するか、ドロップダウン リストからウェルノウン タイプを選択します。
  - Protocol Group：Service Groups で作成されたサービス グループを指定するには、このオプション ボタンをクリックします。ドロップダウン リストからグループ名を選択するか、**...** ボタンをクリックして Browse Service Groups ダイアログボックスを開きます。Browse Service Groups ダイアログボックスでは、サービス グループを追加できます。

Rule Flow Diagram：このルールの Rule Flow Diagram を表示します。この図では、ネットワーク、トラフィックのタイプ、インターフェイス名、フローの方向、およびアクション（Authorize または Do Not Authorize など）を示しています。

Options：このルールのオプションを設定します。

- Time Range：ドロップダウン リストから既存の時間範囲の名前を選択します。時間範囲では、指定した時間だけルールがイネーブルになります。時間範囲は「時間範囲の設定」で作成します。
- Description：このルールの説明を入力します。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

アカウンティング ルールの追加および編集

セキュリティ アプライアンスは、セキュリティ アプライアンスを通過する任意の TCP トラフィックまたは UDP トラフィックについてのアカウンティング情報を RADIUS サーバまたは TACACS+ サーバに送信できます。そのトラフィックも認証されている場合、AAA サーバはユーザ名でアカウンティング情報を保持できます。そのトラフィックが認証されていない場合、AAA サーバは IP アドレスでアカウンティング情報を保持できます。アカウンティング情報には、セッションの開始時刻と終了時刻、ユーザ名、そのセッションでセキュリティ アプライアンスを経由したバイト数、使用されたサービス、セッションの継続時間が含まれます。

フィールド

Interface and Action：インターフェイス、アクション、および AAA サーバ グループを選択します。

- Interface：このルールを適用するインターフェイスを選択します。
- Action：**Account** または **Do not Account** を選択します。
- AAA Server Group：AAA サーバ グループまたはローカル データベースを選択します。Properties > AAA Setup > AAA Server Groups でサーバ グループを追加する必要があります。
- Add Server/User：サーバを選択した AAA サーバ グループに追加するか、ユーザをローカル データベースに追加するには、このボタンをクリックします。

Source：認証するトラフィックの送信元アドレスを指定します。

- Type：any、IP アドレス、Network Object Group、または Interface IP など、使用するアドレスのタイプを選択します。

  IP address を選択した場合、次のフィールドが表示されます。

  - IP Address：手動で入力するか、**...** ボタンをクリックして、Browse Address ダイアログボックスから選択します。
  - Netmask：ドロップダウン リストからサブネット マスクを選択します。

  Network Object Group を選択した場合、次のフィールドが表示されます。

  - Group Name：ドロップダウン リストからグループ名を選択するか、**...** ボタンをクリックして Browse Address ダイアログボックスを開きます。Browse Address ダイアログボックスでは、ネットワーク オブジェクト グループを追加できます。

  Interface IP を選択した場合、次のフィールドが表示されます。

  - Interface：ドロップダウン リストからインターフェイスを選択します。

Destination：アカウンティングするトラフィックの宛先アドレスを指定します。

- Type：any、IP アドレス、Network Object Group、または Interface IP など、使用するアドレスのタイプを選択します。

  IP address を選択した場合、次のフィールドが表示されます。

  - IP Address：手動で入力するか、**...** ボタンをクリックして、Browse Address ダイアログボックスから選択します。
  - Netmask：ドロップダウン リストからサブネット マスクを選択します。

  Network Object Group を選択した場合、次のフィールドが表示されます。

  - Group Name：ドロップダウン リストからグループ名を選択するか、**...** ボタンをクリックして Browse Address ダイアログボックスを開きます。Browse Address ダイアログボックスでは、ネットワーク オブジェクト グループを追加できます。

  Interface IP を選択した場合、次のフィールドが表示されます。

  - Interface：ドロップダウン リストからインターフェイスを選択します。

Protocol and Service：アカウンティングするトラフィックのポートまたはプロトコルを指定します。

- Protocol：tcp または udp の、いずれかのトラフィックのプロトコルを選択します。
  - Source Port：アカウンティングするトラフィックの送信元ポートを設定します。

    Service：ポートまたはポートの範囲を入力するには、このオプション ボタンをクリックします。ドロップダウン リストから、=（等しい）、!=（等しくない）、>（大きい）、<（小さい）などの演算子および範囲を選択します。数字を入力するか、ドロップダウン リストからウェルノウン ポート名を選択します。範囲の場合、数字を指定する必要があります。

    Group：Service Groups で作成されたサービス グループを指定するには、このオプション ボタンをクリックします。ドロップダウン リストからグループ名を選択するか、**...** ボタンをクリックして Browse Service Groups ダイアログボックスを開きます。Browse Service Groups ダイアログボックスでは、サービス グループを追加できます。
  - Destination Port：アカウンティングするトラフィックの宛先ポートを設定します。

    Service：ポートまたはポートの範囲を入力するには、このオプション ボタンをクリックします。ドロップダウン リストから、=（等しい）、!=（等しくない）、>（大きい）、<（小さい）などの演算子および範囲を選択します。数字を入力するか、ドロップダウン リストからウェルノウン ポート名を選択します。範囲の場合、数字を指定する必要があります。

    Group：Service Groups で作成されたサービス グループを指定するには、このオプション ボタンをクリックします。ドロップダウン リストからグループ名を選択するか、**...** ボタンをクリックして Browse Service Groups ダイアログボックスを開きます。Browse Service Groups ダイアログボックスでは、サービス グループを追加できます。

Rule Flow Diagram：このルールの Rule Flow Diagram を表示します。この図では、ネットワーク、トラフィックのタイプ、インターフェイス名、フローの方向、およびアクション（Account または Do Not Account など）を示しています。

Options：このルールのオプションを設定します。

- Time Range：ドロップダウン リストから既存の時間範囲の名前を選択します。時間範囲では、指定した時間だけルールがイネーブルになります。時間範囲は「時間範囲の設定」で作成します。
- Description：このルールの説明を入力します。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

MAC 免除ルールの追加および編集

セキュリティ アプライアンスは、特定の MAC アドレスからのトラフィックの認証および認可を免除できます。

たとえば、セキュリティ アプライアンスが特定のネットワークから発信される TCP トラフィックを認証しても、特定のサーバからの未認証の TCP 接続を許可する場合に、MAC 免除ルールを使用すると、このルールが指定したサーバからのすべてのトラフィックに対して認証および認可が免除されます。

ベスト マッチ シナリオと異なり、パケットは照合する最初のエントリを使用するので、エントリの順番が重要になります。許可エントリがあり、そのエントリにより許可されたアドレスを拒否する場合は、許可エントリの前に拒否エントリを入力してください。

フィールド

- Action : **MAC Exempt** または **No MAC Exempt** を選択します。MAC Exempt オプションでは、認証または認可する必要なく MAC アドレスからのトラフィックを許可します。No MAC Exempt オプションでは、認証または認可を免除しない MAC アドレスを指定します。ffff.ffff.0000 などの MAC アドレス マスクを使用して MAC アドレスの範囲を許可する場合、拒否エントリを追加する必要があります。また、その範囲で認証および認可されるように MAC アドレスを強制します。
- MAC Address : 12 桁の 16 進数の形式（nnnn.nnnn.nnnn）で送信元の MAC アドレスを指定します。
- MAC Mask : 照合に使用される MAC アドレスの一部を指定します。たとえば、ffff.ffff.ffff は完全に MAC アドレスと一致します。ffff.ffff.0000 は最初の 8 桁だけ一致します。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

高度な AAA 機能の設定

Configuration > Security Policy > AAA Rules > Advanced AAA Configuration

Advanced AAA Configuration ダイアログボックスでは、Secure HTTP をイネーブルにし、Proxy Limit を設定して、インタラクティブ認証をイネーブルにできます。

フィールド

- Secure HTTP：Secure HTTP（HTTPS）をイネーブルにするか、ディセーブルにするかを指定します。
- Enable Secure HTTP：Secure HTTP 認証をイネーブルにします。HTTP 認証を保護しないと、クライアントからセキュリティ アプライアンスに送信されるユーザ名およびパスワードは、クリア テキストとして通過します。このオプションをイネーブルにすることで、Web クライアントとセキュリティ アプライアンスとの間で HTTPS を使用して行われるユーザ名とパスワードの交換がイネーブルになります。この機能をイネーブルにした後、ユーザが HTTP を使用しているときに認証を必要とした場合は、セキュリティ アプライアンスが HTTP ユーザを HTTPS プロンプトにリダイレクトします。正常に認証されると、セキュリティ アプライアンスにより元の HTTP URL にリダイレクトされます。
- Proxy Limit：Proxy Limit パラメータを指定します。
  - Enable Proxy Limit：ユーザごとに許可される同時プロキシ接続の数を制限します。最大接続数は 128 です。この機能をイネーブルにしない場合、制限なしになります。
  - Proxy Limit：許可される同時プロキシ接続の数を指定します。指定できる値は 1 ～ 128、デフォルトは 16 です。
- Interactive Authentication：HTTP および HTTPS トラフィックのインタラクティブ認証を設定します。デフォルトでは、インライン基本認証が使用されます。また、この領域では、直接認証も設定されます。インタラクティブ認証の詳細については、P.19-14 の「インタラクティブ認証ルールの追加」を参照してください。
  - Interface：インタラクティブ認証をイネーブルにしたインターフェイスを表示します。
  - Protocol：HTTP または HTTPS のプロトコルを表示します。
  - Port：受信ポートを表示します。
  - Redirect：通過トラフィックのリダイレクションをイネーブルにしたかどうかを表示します。リダイレクションなしの場合、このルールでは直接認証だけがイネーブルになります。
  - Add：インタラクティブ認証ルールを追加します。
  - Edit：インタラクティブ認証ルールを編集します。
  - Delete：インタラクティブ認証ルールを削除します。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

インタラクティブ認証ルールの追加

HTTP のデフォルトでは、セキュリティ アプライアンスは基本 HTTP 認証を使用します。HTTPS の場合、セキュリティ アプライアンスは同様のカスタム ログイン画面を生成します。Configuration > Security Policy > AAA Rules > Advanced AAA Configuration > Add Interactive Authentication ダイアログボックスを使用すれば、ユーザがユーザ名とパスワードを入力できる内部 Web ページにセキュリティ アプライアンスがユーザをリダイレクトするように設定できます。

HTTP および HTTPS 認証のリダイレクト方式をイネーブルにした場合、セキュリティ アプライアンスでの直接認証も自動的にイネーブルになります。HTTP、HTTPS、Telnet、または FTP によるセキュリティ アプライアンスの通過は許可しないが他のタイプのトラフィックは認証する場合、直接認証は役に立ちます。他のトラフィックが許可される前に、ユーザは HTTP または HTTPS を使用するセキュリティ アプライアンスを直接認証できます。通過トラフィックに基本 HTTP 認証を引き続き使用する場合、直接認証は独立して設定できます。直接認証のログイン ページにアクセスするには、次の URL のいずれかを入力します。

http://*interface_ip*[**:***port*]**/netaccess/connstatus.html**
https://*interface_ip*[**:***port*]**/netaccess/connstatus.html**

リダイレクションは、基本方式を強化したものです。これは、認証時に向上したユーザ エクスペリエンスが提供されると同時に、Easy VPN でもファイアウォール モードでも、HTTP および HTTPS と同じユーザ エクスペリエンスが提供されるためです。また、セキュリティ アプライアンスでの直接認証もサポートしています。

基本 HTTP 認証を引き続き使用するのは、セキュリティ アプライアンスに受信ポートを開かせない場合、ルータで NAT を使用し、セキュリティ アプライアンスが提供する Web ページの変換ルールを作成しない場合、および使用ネットワークで基本 HTTP 認証が動作に適している場合です。たとえば、URL が埋め込まれている電子メールなどブラウザ以外のアプリケーションは、基本認証との互換性が高くなっています。

インタラクティブ認証ルールを設定するには、次の手順を実行します。

ステップ 1　Configuration > Security Policy > AAA Rules > Advanced AAA Configuration ダイアログボックスで **Add** をクリックします。

ステップ 2　Protocol メニューから、**HTTP** または **HTTPS** を選択します。

HTTP と HTTPS の両方のリスナをイネーブルにするには、2 つの別のルールを作成する必要があります。

ステップ 3　Interface メニューから、リスナをイネーブルにするインターフェイス名を選択します。

ステップ 4　Port メニューから共通ポートを選択するか、リスンするポート番号を入力します。

HTTP のデフォルトは 80、HTTPS のデフォルトは 443 です。

ステップ 5　通過トラフィックを認証用の受信ポートにリダイレクトするには、**Redirect network users for authentication requests** チェックボックスをオンにします。

このチェックボックスをオンにしない場合、直接認証だけがイネーブルになります。

ステップ 6　**OK** をクリックします。

フィールド

- Protocol：インタラクティブ認証ルールのプロトコルを HTTP または HTTPS に設定します。
- Interface：受信ポートをイネーブルにするインターフェイス名を設定します。
- Port：リスンするポート番号を設定します。 共通ポートを選択するか、ポート番号を入力します。HTTP のデフォルトは 80、HTTPS のデフォルトは 443 です。
- Redirect network users for authentication requests：通過トラフィックを認証用の受信ポートにリダイレクトします。このチェックボックスをオンにしない場合、直接認証だけがイネーブルになります。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

認可のための RADIUS サーバの設定

認証が成功すると、RADIUS プロトコルは RADIUS サーバによって送信される access-accept メッセージでユーザ認可を返します。

ネットワーク アクセスについてユーザを認証するようにセキュリティ アプライアンスを設定すると、RADIUS 認可も暗黙的にイネーブルになっています。したがって、この項では、セキュリティ アプライアンス上の RADIUS 認可の設定については取り上げません。ここでは、セキュリティ アプライアンスが RADIUS サーバから受信したアクセスリスト情報をどのように処理するかについて説明します。

アクセスリストをセキュリティ アプライアンスにダウンロードするように RADIUS サーバを設定できます。または、認証時にアクセスリスト名をダウンロードするようにも設定できます。ユーザは、ユーザ固有のアクセスリストで許可された操作だけを認可されます。

（注）　**access-group** コマンドを使用してアクセスリストをインターフェイスに適用した場合は、**per-user-override** キーワードが、ユーザ固有のアクセスリストによる認可に対して次のように影響を与えることに注意してください。

- **per-user-override** キーワードを使用しない場合、ユーザ セッションのトラフィックは、インターフェイス アクセスリストとユーザ固有のアクセスリストの両方によって許可される必要があります。
- **per-user-override** キーワードを使用した場合、ユーザ固有のアクセスリストによって許可される内容が決定されます。

詳細については、『*Cisco Security Appliance Command Reference*』の **access-group** コマンドの項を参照してください。

この項は、次の内容で構成されています。

ダウンロード可能な ACL を送信するための RADIUS サーバの設定

この項では、Cisco Secure ACS およびサードパーティ RADIUS サーバを設定する方法について説明します。次の項目を取り上げます。

ダウンロード可能なアクセスリストの機能と Cisco Secure ACS について

ダウンロード可能なアクセスリストは、Cisco Secure ACS を使用して各サーバに適切なアクセスリストを提供する場合に最もスケーラブルな方法です。次の機能があります。

- 無制限のアクセスリスト サイズ：ダウンロード可能なアクセスリストは、完全なアクセスリストを Cisco Secure ACS からセキュリティ アプライアンスに転送するために必要な数の RADIUS パケットを使用して送信されます。

- アクセスリスト管理の簡素化および集中化：ダウンロード可能なアクセスリストにより、一度記述したアクセスリスト セットを多数のユーザ プロファイルまたはグループ プロファイルに適用することや、多数のセキュリティ アプライアンスに配布することができます。

この方法は、複数の Cisco Secure ACS ユーザまたはグループに適用する非常に大きいアクセスリスト セットがある場合に最適ですが、Cisco Secure ACS ユーザおよびグループの管理を簡素化できることから、アクセスリストのサイズを問わず有用です。

セキュリティ アプライアンスは、ダウンロード可能なアクセスリストを Cisco Secure ACS から次のプロセスで受信します。

1. セキュリティ アプライアンスがユーザ セッションのための RADIUS 認証要求パケットを送信します。
2. Cisco Secure ACS がそのユーザを正常に認証した場合、Cisco Secure ACS は、該当するダウンロード可能なアクセスリストの内部名が含まれた RADIUS access-accept メッセージを返します。Cisco IOS cisco-av-pair RADIUS VSA（ベンダー 9、アトリビュート 1）には、ダウンロード可能なアクセスリスト セットを特定する次の AV のペアが含まれています。

   ```
   ACS:CiscoSecure-Defined-ACL=acl-set-name
   ```

   acl-set-name はダウンロード可能なアクセスリストの内部名です。この名前は、Cisco Secure ACS 管理者がアクセスリストに割り当てた名前とアクセスリストが最後に変更された日時の組み合せです。
3. セキュリティ アプライアンスはダウンロード可能なアクセスリストの名前を検査し、以前にその名前のダウンロード可能なアクセスリストを受信したことがあるかどうかを判別します。
   - セキュリティ　アプライアンスが以前にその名前のダウンロード可能アクセスリストを受信したことがある場合は、Cisco Secure ACS との通信は完了し、セキュリティ アプライアンスはアクセスリストをユーザ セッションに適用します。ダウンロード可能なアクセスリストの名前には最後に変更された日時が含まれているため、Cisco Secure ACS から送信された名前と、以前にダウンロードしたアクセスリストの名前が一致するということは、セキュリティ アプライアンスはダウンロード可能なアクセスリストの最新バージョンを持っていることになります。
   - セキュリティ　アプライアンスが以前にその名前のダウンロード可能なアクセスリストを受信したことがない場合は、そのアクセスリストの古いバージョンを持っているか、そのアクセスリストのどのバージョンもダウンロードしたことがないことになります。いずれの場合でも、セキュリティ アプライアンスは、ダウンロード可能なアクセスリスト名を RADIUS 要求内のユーザ名として使用し、ヌル パスワード アトリビュートとともに RADIUS 認証要求を発行します。cisco-av-pair RADIUS VSA では、この要求に次の AV のペアも含まれます。

     ```
     AAA:service=ip-admission
     AAA:event=acl-download
     ```

     これに加えて、セキュリティ アプライアンスは Message-Authenticator アトリビュート（IETF RADIUS アトリビュート 80）で要求に署名します。
4. ダウンロード可能なアクセスリストの名前が含まれているユーザ名アトリビュートを持つ RADIUS 認証要求を受信すると、Cisco Secure ACS は Message-Authenticator アトリビュートをチェックして要求を認証します。Message-Authenticator アトリビュートがない場合、または正しくない場合、Cisco Secure ACS はその要求を無視します。Message-Authenticator アトリビュートの存在により、ダウンロード可能なアクセスリスト名がネットワーク アクセスの不正取得に悪用されることが防止されます。Message-Authenticator アトリビュートとその使用方法は、RFC 2869「RADIUS Extensions」で定義されています。この文書は、http://www.ietf.org で入手できます。
5. 要求されたアクセスリストの長さが約 4 KB 未満の場合、Cisco Secure ACS はそのアクセスリストを含めた access-accept メッセージで応答します。メッセージには他の必須アトリビュートを含める必要があるので、1 つの access-accept メッセージに収まるアクセスリストの最大サイズは 4 KB よりわずかに小さくなります。

Cisco Secure ACS はダウンロード可能なアクセスリストを cisco-av-pair RADIUS VSA で送信します。アクセスリストは、一連の AV のペアという形式をとります。各ペアには ACE が 1 つ含まれ、シリアル番号が付けられます。

```
ip:inacl#1=ACE-1
ip:inacl#2=ACE-2
.
.
.
ip:inacl#n=ACE-n
```

AV のペアの例を次に示します。

```
ip:inacl#1=permit tcp 10.1.0.0 255.0.0.0 10.0.0.0 255.0.0.0
```

6. 要求されたアクセスリストの長さが約 4 KB を超える場合、Cisco Secure ACS は、上記の形式のアクセスリストの一部が含まれた access-challenge メッセージで応答します。メッセージには、State アトリビュート（IETF RADIUS アトリビュート 24）も含まれています。State アトリビュートには、Cisco Secure ACS がダウンロードの進捗を追跡するために使用する制御データが含まれています。Cisco Secure ACS は、RADIUS メッセージの最大サイズ以内で可能な限り多数の完全な AV のペアを cisco-av-pair RADIUS VSA に含めます。

   セキュリティ アプライアンスはアクセスリストの一部を受信すると、それを保存し、新しい access-request メッセージで応答します。これには、ダウンロード可能なアクセスリストを求める最初の要求と同じアトリビュートと、access-challenge メッセージで受信した State アトリビュートのコピーが含まれています。

   これは、Cisco Secure ACS がアクセスリストの最後の部分を access-accept メッセージで送信するまで続行されます。

ダウンロード可能なアクセスリストに関する Cisco Secure ACS の設定

Cisco Secure ACS 上のダウンロード可能なアクセスリストを共有プロファイル コンポーネントとして設定し、そのアクセスリストをグループまたは個々のユーザに割り当てることができます。

アクセスリスト定義は、次のプレフィックスがない点を除いて拡張 **access-list** コマンドに類似する、1 つまたは複数のセキュリティ アプライアンス コマンドで構成されます。

access-list *acl_name* **extended**

Cisco Secure ACS バージョン 3.3 上のダウンロード可能なアクセスリスト定義の例を次に示します。

```
+-------------------------------------------+
| Shared profile Components                 |
|                                           |
|      Downloadable IP ACLs Content         |
|                                           |
| Name:    acs_ten_acl                      |
|                                           |
|      ACL Definitions                      |
|                                           |
| permit tcp any host 10.0.0.254            |
| permit udp any host 10.0.0.254            |
| permit icmp any host 10.0.0.254           |
| permit tcp any host 10.0.0.253            |
| permit udp any host 10.0.0.253            |
| permit icmp any host 10.0.0.253           |
| permit tcp any host 10.0.0.252            |
| permit udp any host 10.0.0.252            |
| permit icmp any host 10.0.0.252           |
| permit ip any any                         |
+-------------------------------------------+
```

ダウンロード可能なアクセスリストを作成する方法、およびそれらをユーザと関連付ける方法の詳細については、ご使用のバージョンの Cisco Secure ACS のマニュアルを参照してください。

セキュリティ アプライアンス上では、ダウンロードされたアクセスリストの名前は次のようになります。

```
#ACSACL#-ip-acl_name-number
```

acl_name 引数は Cisco Secure ACS で定義された名前（上記の例では acs_ten_acl）、*number* は Cisco Secure ACS が生成した一意のバージョン ID です。

セキュリティ アプライアンス上にダウンロードされたアクセスリストは、次の行で構成されます。

```
access-list #ACSACL#-ip-asa-acs_ten_acl-3b5385f7 permit tcp any host 10.0.0.254
access-list #ACSACL#-ip-asa-acs_ten_acl-3b5385f7 permit udp any host 10.0.0.254
access-list #ACSACL#-ip-asa-acs_ten_acl-3b5385f7 permit icmp any host 10.0.0.254
access-list #ACSACL#-ip-asa-acs_ten_acl-3b5385f7 permit tcp any host 10.0.0.253
access-list #ACSACL#-ip-asa-acs_ten_acl-3b5385f7 permit udp any host 10.0.0.253
access-list #ACSACL#-ip-asa-acs_ten_acl-3b5385f7 permit icmp any host 10.0.0.253
access-list #ACSACL#-ip-asa-acs_ten_acl-3b5385f7 permit tcp any host 10.0.0.252
access-list #ACSACL#-ip-asa-acs_ten_acl-3b5385f7 permit udp any host 10.0.0.252
access-list #ACSACL#-ip-asa-acs_ten_acl-3b5385f7 permit icmp any host 10.0.0.252
access-list #ACSACL#-ip-asa-acs_ten_acl-3b5385f7 permit ip any any
```

ダウンロード可能なアクセスリストに関する任意の RADIUS サーバの設定

ユーザ固有のアクセスリストを Cisco IOS RADIUS cisco-av-pair VSA（ベンダー 9、アトリビュート 1）でセキュリティ アプライアンスに送信するように、Cisco IOS RADIUS VSA をサポートする任意の RADIUS サーバを設定できます。

cisco-av-pair VSA で、**access-list extended** コマンドと類似する 1 つまたは複数の ACE を設定します。ただし、次のコマンド プレフィックスを置き換える必要があります。

access-list *acl_name* **extended**

次のテキストに置き換えます。

ip:inacl#*nnn***=**

nnn 引数は、0 ～ 999999999 の番号で、セキュリティ アプライアンス上に設定するコマンド文の順序を指定します。このパラメータを省略すると、順番は 0 となり、cisco-av-pair RADIUS VSA 内部の ACE の順序が使用されます。

RADIUS サーバ上の cisco-av-pair VSA に対して設定されている必要のあるアクセスリスト定義の例を次に示します。

```
ip:inacl#1=permit tcp 10.1.0.0 255.0.0.0 10.0.0.0 255.0.0.0
ip:inacl#99=deny tcp any any
ip:inacl#2=permit udp 10.1.0.0 255.0.0.0 10.0.0.0 255.0.0.0
ip:inacl#100=deny udp any any
ip:inacl#3=permit icmp 10.1.0.0 255.0.0.0 10.0.0.0 255.0.0.0
```

cisco-av-pair アトリビュートで送信されるアクセスリストをユーザごとに一意にする方法については、ご使用の RADIUS サーバのマニュアルを参照してください。

セキュリティ アプライアンス上では、ダウンロードされたアクセスリストの名前は次の形式になります。

```
AAA-user-username
```

username 引数は、認証を受けるユーザの名前です。

セキュリティ アプライアンス上にダウンロードされたアクセスリストは、次の行で構成されます。RADIUS サーバ上で指定された番号に基づいた順序になっています。

```
access-list  AAA-user-bcham34-79AD4A08 permit tcp 10.1.0.0 255.0.0.0 10.0.0.0 255.0.0.0
access-list  AAA-user-bcham34-79AD4A08 permit udp 10.1.0.0 255.0.0.0 10.0.0.0 255.0.0.0
access-list  AAA-user-bcham34-79AD4A08 permit icmp 10.1.0.0 255.0.0.0 10.0.0.0 255.0.0.0
access-list  AAA-user-bcham34-79AD4A08 deny tcp any any
access-list  AAA-user-bcham34-79AD4A08 deny udp any any
```

ダウンロードされたアクセスリストの「access-list」という単語と名前の間には、2 個のスペースがあります。これらのスペースにより、ダウンロードされたアクセスリストとローカルのアクセスリストが区別されます。この例では、「79AD4A08」はセキュリティ アプライアンスが作成したハッシュ値で、RADIUS サーバ上でアクセスリスト定義がいつ変更されたかを判別するために役立ちます。

ダウンロード可能なアクセスリスト内のワイルドカード ネットマスク表現の変換

RADIUS サーバを使用して、ダウンロード可能なアクセスリストを Cisco VPN 3000 Series Concentrator およびセキュリティ アプライアンスに提供する場合は、ワイルドカード ネットマスク表現を標準のネットマスク表現に変換するようにセキュリティ アプライアンスを設定しなければならない場合があります。これは、Cisco VPN 3000 Series Concentrator はワイルドカード ネットマスク表現をサポートしますが、セキュリティ アプライアンスは標準のネットマスク表現しかサポートしないためです。これらの違いは、RADIUS サーバ上のダウンロード可能なアクセスリストを設定する方法に影響しますが、ワイルドカード ネットマスク表現を変換するようにセキュリティ アプライアンスを設定することで、その影響を最小限に抑えることができます。ワイルドカード ネットマスク表現の変換により、RADIUS サーバ上のダウンロード可能なアクセスリストのコンフィギュレーションを変更することなく、Cisco VPN 3000 Series Concentrator 用に記述されたダウンロード可能なアクセスリストをセキュリティ アプライアンスで使用できます。

アクセスリスト ネットマスク変換は、**acl-netmask-convert** コマンドを使用してサーバごとに設定できます。このコマンドは aaa サーバ コンフィギュレーション モードで使用できます。RADIUS サーバの設定方法の詳細については、「AAA のセットアップ」を参照してください。**acl-netmask-convert** コマンドの詳細については、『*Cisco Security Appliance Command Reference*』を参照してください。

ユーザごとの ACL 名をダウンロードするための RADIUS サーバの設定

ユーザ認証時に、セキュリティ アプライアンスで作成済みのアクセスリストの名前を RADIUS サーバからダウンロードするには、IETF RADIUS filter-id アトリビュート（アトリビュート番号 11）を次のように設定します。

filter-id=*acl_name*

（注）　Cisco Secure ACS では、filter-id アトリビュートの値は、HTML インターフェイスのボックスで、**filter-id=** を省略し、*acl_name* だけを入力して指定します。

filter-id アトリビュートの値をユーザごとに一意にする方法については、ご使用の RADIUS サーバのマニュアルを参照してください。